

ESTTA Tracking number: **ESTTA1074901**

Filing date: **08/13/2020**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Petition for Cancellation

Notice is hereby given that the following party has filed a petition to cancel the registration indicated below.

Petitioner Information

Name	CrowdStrike, Inc.		
Entity	Corporation	Citizenship	Delaware
Address	15440 LAGUNA CANYON ROAD, SUITE 250 IRVINE, CA 92618 UNITED STATES		
Attorney information	CARLA B. OAKLEY MORGAN, LEWIS & BOCKIUS LLP ONE MARKET, SPEAR STREET TOWER SAN FRANCISCO, CA 94105 UNITED STATES Primary Email: carla.oakley@morganlewis.com Secondary Email(s): jenna.stokes@morganlewis.com, rtyz@tyzlaw.com, ejones@tyzlaw.com, sftrademarks@morganlewis.com 415-442-1301		
Docket Number			

Registration Subject to Cancellation

Registration No.	3320549	Registration date	10/23/2007
Registrant	Fair Isaac Corporation 181 METRO DRIVE SAN JOSE, MN 95110 UNITED STATES		

Goods/Services Subject to Cancellation

Class 009. First Use: 1992/00/00 First Use In Commerce: 1992/00/00 All goods and services in the class are subject to cancellation, namely: Software and enterprise software applications for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card fraud, check fraud, identity theft, mortgage fraud, and banking fraud
Class 042. First Use: 1992/00/00 First Use In Commerce: 1992/00/00 All goods and services in the class are subject to cancellation, namely: Providing temporary use of online non-downloadable software for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card fraud, identity theft, mortgage fraud, and banking fraud; and development of customized software for others for use in monitoring, tracking, detecting, preventing and managing fraud
Class 045. First Use: 1992/00/00 First Use In Commerce: 1992/00/00 All goods and services in the class are subject to cancellation, namely: Fraud detection services using data warehousing, data mining and predictive modeling software, all for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card

fraud, check fraud, identity theft, mortgage fraud, and banking fraud

Grounds for Cancellation

Abandonment	Trademark Act Section 14(3)
-------------	-----------------------------

Related Proceedings	91231416, 92064876, 92070142
---------------------	------------------------------

Attachments	Petition to Cancel 549 Registration.pdf(1552162 bytes) Petition to Cancel 549 Registration - Exhibits.pdf(5758538 bytes)
-------------	---

Signature	/s/ Carla B. Oakley
Name	Carla B. Oakley
Date	08/13/2020

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner,

v.

FAIR ISAAC CORPORATION
Respondent.

In re Registration No. 3320549

Cancellation No. _____

PETITION FOR CANCELLATION

In this Petition, CrowdStrike seeks under Sections 14 and 18 of the Lanham Act, 15 U.S.C. §§ 1064 and 1068 cancellation of Fair Isaac Corporation’s (“FICO”) Registration No. 3320549 for the mark FALCON (the “’549 Registration”) on the grounds of abandonment. CrowdStrike has standing to bring this Petition because FICO is currently challenging two registrations and one application owned by CrowdStrike (Opposition No. 91231416 (Parent) and Cancellation Action No. 92064876), based on FICO’s ’549 Registration.¹

As grounds for this Petition, CrowdStrike alleges the following:

CrowdStrike’s CROWDSTRIKE FALCON and FALCON OVERWATCH Marks

1. Since 2011, CrowdStrike has been an industry leader in computer and network security technology and services utilizing its proprietary endpoint protection technology. Its CROWDSTRIKE FALCON[®] platform’s single lightweight-agent architecture leverages cloud-

¹ CrowdStrike moved to add this claim to Cancellation No. 92070142, which is consolidated with Opposition No. 91231416. In the August 3, 2020, order ruling on that motion (issued in Opposition No. 91231416), CrowdStrike was instructed instead to file a separate petition to cancel the ’549 Registration or a motion for leave to amend to assert a counterclaim in Opposition No. 91231416 or Cancellation No. 92070142. Order at 5. To avoid any delay that may be caused by first filing a motion to amend, CrowdStrike is filing this separate petition.

scale artificial intelligence (AI) and offers real time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network.

2. CrowdStrike owns two federal registrations for its CROWDSTRIKE FALCON mark. (Copies of the registration certificates are attached as **Exhibit A.**)

3. CrowdStrike's U.S. Registration No. 4629491 (the "'491 Registration") for CROWDSTRIKE FALCON, issued October 28, 2014, covers:

Class 9: Downloadable computer software for computer and network security.

Class 45: Monitoring of computer systems for security purposes; provision of systems for the management of computer and network threats, namely, surveillance and monitoring of vulnerability and security problems in computer hardware, networks, and software; implementing plans for improving computer and network security for businesses and governmental agencies, namely, computer security assurance, administration of digital keys and digital certificates, providing fraud detection services for electronic funds transfer, and credit and debit card and electronic check transactions via a global computer network.

4. CrowdStrike's U.S. Registration No. 4720653 (the "'653 Registration") for CROWDSTRIKE FALCON, issued April 14, 2015, covers:

Class 42: Computer consultation; consulting in the field of information technology; computer consultation in the field of computer and network security; computer security consultancy in the field of scanning and penetration testing of computers and networks to assess information security vulnerability; software as a service (SAAS) services featuring software in the field of computer and network security; software as a service (SAAS) services, namely, hosting software for use by others for detecting, blocking, and removing computer viruses and threats; application service provider (ASP) featuring non-downloadable computer software for use in computer and network security; maintenance and updating of computer software relating to computer and network security and prevention of computer risks; computer security consultancy, namely, developing plans for improving computer and network security for businesses and governmental agencies; cloud computing featuring software for use in computer and network security; cloud computing services in the field of computer and network security; computer services, namely, acting as an application service provider in the field of knowledge management to host computer application software for creating databases of information and data related to malware and computer and network security; computer services, namely, online scanning, detecting, quarantining, and eliminating viruses, worms, Trojans, spyware, adware, malware and unauthorized data and programs on computers, networks, and electronic devices; computer

systems analysis; implementing plans for improving computer and network security and preventing criminal activity for businesses and governmental agencies, namely, identifying malware on computer systems, identifying the source and genealogy of malware, and identifying the objectives of computer system attackers.

5. FICO admits that it learned of CrowdStrike's use of the CROWDSTRIKE FALCON mark at least as early as May 2014, and filed its petition to cancel CrowdStrike's '491 Registration and '653 Registration more than two years later, in November 2016. FICO's petition to cancel is based, in part, on the '549 Registration and remains pending (Cancellation No. 92070142).

6. CrowdStrike filed an application for the mark FALCON OVERWATCH on February 19, 2016, Serial No. 86913839. FICO opposed that application, citing its '549 Registration. The opposition remains pending (Opposition No. 91231416). Although the application was filed on an "intent to use" basis, CrowdStrike started using its FALCON OVERWATCH mark at least as early as February 2016 for certain services identified in the application.

7. CrowdStrike has invested significantly in advertising and promoting its products and services using its CROWDSTRIKE FALCON mark and its FALCON OVERWATCH mark. CrowdStrike's customer base tripled in 2014. By February 2015, CrowdStrike ranked in the Top 100 High-Growth privately held U.S. companies by Forbes.

FICO's '549 Registration

8. On October 20, 2005, FICO filed its intent-to-use application Serial No. 78733833 for the mark FALCON that ultimately matured into the '549 Registration.

9. On November 14, 2006, the United States Patent and Trademark Office (“USPTO”) allowed the application that matured into the ’549 Registration, resulting in a statement of use deadline of May 14, 2006.

10. On May 14, 2007, FICO filed a Statement of Use stating that the FALCON mark was in use in connection with all of the goods and services covered by the application and had been since 1992.

11. The ’549 Registration issued on October 23, 2007, covering the following goods and services:

Class 9: Software and enterprise software applications for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card fraud, check fraud, identity theft, mortgage fraud, and banking fraud.

Class 42: Providing temporary use of online non-downloadable software for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card fraud, identity theft, mortgage fraud, and banking fraud; and development of customized software for others for use in monitoring, tracking, detecting, preventing and managing fraud.

Class 45: Fraud detection services using data warehousing, data mining and predictive modeling software, all for use in monitoring, tracking, detecting, preventing and managing fraud in the fields of credit fraud, credit card fraud, debit card fraud, check fraud, identity theft, mortgage fraud, and banking fraud.

FICO Abandons the FALCON Mark

12. In discovery in the consolidated Opposition No. 91231416 and Cancellation No. 92064876 proceedings, CrowdStrike requested documents (including Request Nos. 50 and 75) showing, among other things, FICO’s use of the FALCON mark, agreements pertaining to enforcement of its rights, and documents showing third party usage of marks that include or consist of the term FALCON. FICO’s document production did not include documents reflecting third-party use of the FALCON mark for financial fraud monitoring services, or any license agreements with third parties authorizing the use of the FALCON mark for financial

fraud monitoring products or services. FICO did not assert objections justifying the withholding of such documents, nor would such objections have been reasonable. In response to a request for admission regarding third party usages (RFA No. 59), FICO admitted that it was aware of third party usages of “Falcon” that it was pursuing through enforcement activity, but made no mention of licensed third party usage.

13. CrowdStrike’s own investigation uncovered that a number of third parties, including at least thirty financial institutions, have been and are using “Falcon” to promote services and software such as those described in the ’549 Registration for the mark FALCON since at least as early as 2014.

14. This array of third-party uses of “Falcon” by a variety of financial institutions describing products and services the same or similar to those in the ’549 Registration has resulted in the loss of significance of FALCON as a trademark.

15. For example, the SF Police Credit Union website that previously was available at <https://www.sfpcu.org/accounts-services/convenience-services/falcon-fraud-manager>, stated that “[w]e offer Falcon Fraud Manager to enhance the security of your electronic transactions,” as part of an upgrade to “[o]ur fraud detection system” which generates notifications from “our automated assistant”):



Online Banking Login



Home > Accounts & Services > Convenience Services >
[Falcon Fraud Manager](#)

Falcon Fraud Manager

A A A

At SFPCU, we are committed to protecting your personal information so you can use your SFPCU MasterCard® Debit Card and Visa® Credit Card with confidence. We offer Falcon Fraud Manager to enhance the security of your electronic transactions with a system that detects fraud quickly and accurately to minimize your risk and protect against losses.

[Contact Us Now](#)


Automated Debit Card Fraud Detection and Notification System

Our fraud detection system will be upgraded starting April 15, 2015. The new system will notify you faster when suspected fraud is detected on your SFPCU Debit card.

Starting April 15, if possible fraud is detected on your account, you'll receive a notification call from our automated assistant. If you receive one of these calls, please work with the automated assistant to answer questions regarding recent card activity.

- If the recent activity is legitimate, you will be able to close the case using your touch-tone phone.
- If suspicious transactions are identified as fraudulent, your call will be transferred to Card Member Security to help you protect your cards.

16. The URL identified in paragraph 15 now redirects to the Police Credit Union website at <https://www.thepolicecu.org/accounts-services/convenience-services/falcon-fraud-manager>, which continues to promote a Falcon Fraud Manager offering in the same manner:



ONLINE BANKING LOGIN

Forgot Password | Forgot Login ID | Not a Current Online Banking User? | Login Help

Search Contact Us Find a Branch or ATM

APPLY NOW: Consumer Loan | HELOC | Membership | Home Loan

Accounts & Services

Online Services

Investment Services

Insurance


Membership

About Us

Education Center

Security

Switch to The Police Credit Union



Home > Accounts & Services > Convenience Services > Falcon Fraud Manager

Falcon Fraud Manager

A A A

At The Police Credit Union, we are committed to protecting your personal information so you can use your MasterCard® Debit Card and Visa® Credit Card with confidence. We offer Falcon Fraud Manager to enhance the security of your electronic transactions with a system that detects fraud quickly and accurately to minimize your risk and protect against losses.

Contact Us Now

Automated Debit Card Fraud Detection and Notification System

Our fraud detection system will be upgraded starting April 15, 2015. The new system will notify you faster when suspected fraud is detected on your Police Credit Union Debit card.

Starting April 15, if possible fraud is detected on your account, you'll receive a notification call from our automated assistant. If you receive one of these calls, please work with the automated assistant to answer questions regarding recent card activity.

- If the recent activity is legitimate, you will be able to close the case using your touch-tone phone.
- If suspicious transactions are identified as fraudulent, your call will be transferred to Card Member Security to help you protect your cards.

24-Hour Monitoring

Falcon Fraud Manager monitors signature-based and PIN-based transactions 24 hour a day, seven days a week.

- Each debit and credit card transaction is assigned a score on a risk-based scale.
- High-risk transactions will trigger Falcon Fraud Manager to contact you to determine the transaction's legitimacy.
- If the score is deemed ultra-risky, Falcon Fraud Manager may block your account temporarily if you can't be reached, in order to secure the card against fraudulent activity.

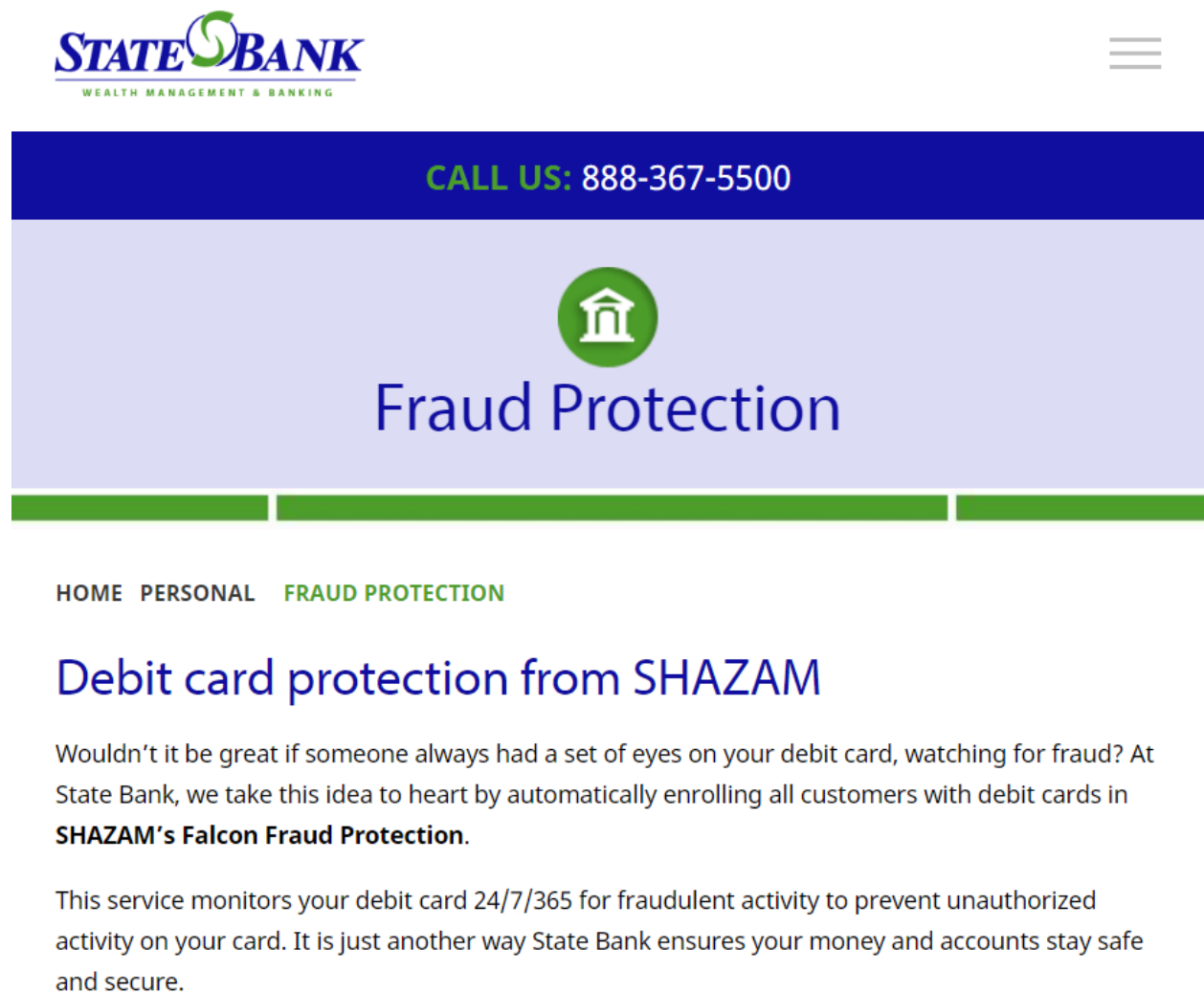
Even with Falcon Fraud Manager, you should contact The Police Credit Union immediately if the following occurs:

- You suspect your card has been compromised.
- Your contact information has changed. (It's vital to keep your contact information and emergency contact information current at The Police Credit Union.)
- You are planning a vacation and know there will be unusual activity on your card.

To learn more about Falcon Fraud and to report suspicious activity on your debit or credit card, contact The Police Credit Union at 800.222.1391.

Report a Blocked, Lost, or Stolen Card

17. Other third-party uses of “Falcon” indicate that a separate third party is the source of the services offered under a “Falcon” designation and described in the ’549 Registration. For example, the State Bank website, previously available at <https://www.statebankia.com/banking/personal/fraud>, referred to “*SHAZAM*’s Falcon Fraud Protection” (emphasis added):



18. The URL provided in paragraph 17, above, now redirects to a website for Fidelity Bank & Trust. That website states that, as of October 14, 2019, Community State Bank was merged into Fidelity Bank & Trust. The Fidelity Bank & Trust website, like the State Bank

website, promotes “Falcon Fraud Alerts” that appear to be part of Shazam Bolt\$. “Not only do we provide our customers with access to Shazam Bolt\$, but a recent update to our Falcon Fraud Alerts now allows customers, who have a mobile phone connected to their account, to receive fraud alerts via text message.” This statement is found at <https://www.bankfidelity.bank/media-events/blog/shazam-bolt-get-alerts-about-potential-fraud>, as shown in the screen shot below:

Shazam Bolt\$: Get Alerts About Potential Fraud

This app protects you in so many ways!

Here at Fidelity Bank & Trust we are proud to offer our neighbors access to Shazam Bolt\$ - the free mobile app that alerts you of potential fraud! Available for download through Google Play and the App Store, this app protects you in so many ways.

- Catch and reduce fraud
- Save money and time
- Provide your cardholders more control over their accounts
- Promote brand awareness
- Set alerts and blocks at the transaction level

“Customers are not only able to easily login and view transaction history, they can actually set up a variety of alerts for themselves. For example, they can choose to receive an alert in the event of an international transaction or even choose to receive an alert everytime a transaction is over a certain dollar amount. They can also pause their card directly on the app, instead of calling Shazam to cancel it altogether,” says Mary Behnken, Assistant Vice President.

Living in a mobile world with sophisticated technology Fidelity Bank & Trust strives to make banking as functional as possible. Not only do we provide our customers with access to Shazam Bolt\$, but a recent update to our Falcon Fraud Alerts now allows customers, who have a mobile phone connected to their account, to receive fraud alerts via text message.

“Things are becoming more and more instant, day by day and we, as a bank, are proud to be growing right along with this trend,” says Mary. “Even our older generation likes that these user-friendly features are available.”

Mary adds the team at Fidelity Bank & Trust is more than happy to explain the features of Shazam Bolt\$ to customers. They’ll even help you set up alerts within the app!

This app is incredibly helpful and gives you all the convenience and control over your accounts. If you want to learn more about it, give us a call or download the app today on Google Play or the App Store.



19. The Iowa State Bank website at <https://www.iowastatebank.net/personal/debit-cards> also promotes a debit card protection service called “Falcon,” describing it as follows:

What is Falcon?

Falcon is a fraud prevention software from SHAZAM, our debit card provider that helps identify and reduce fraud risk by detecting potentially fraudulent PIN-based and signature-based debit transactions. It has a proven reputation of helping minimize payment card fraud losses.

What happens if Falcon detects fraudulent activity on my debit card?

SHAZAM Fraud Specialist will call you if any suspicious activity is detected on your account. They will identify themselves as SHAZAM, calling on behalf of Iowa State Bank.

20. Likewise, as shown in the screen shot below, the Marion County Bank promotes the Brella by Shazam app as a “line of defense against debit card fraud” and advises consumers: “When you are aware of suspicious activity, you can contact Marion County Bank or Shazam Falcon Fraud Manager sooner.”

The screenshot displays the Marion County Bank website. At the top, the bank's logo is on the left, and navigation links for PERSONAL, BUSINESS, AGRICULTURE, MAIN STREET ADVISORY GROUP, and ABOUT US are on the right. The main content area features a section titled "BRELLA BY SHAZAM". Below this title, it states: "The Brella app provides another line of defense against debit card fraud." and "This app allows you to:" followed by a list of features: "Receive notifications of potential fraudulent activities", "Set blocks on specific transactions", "Freeze your card if lost or stolen", and "Locate nearby ATMs wherever you are". It then says "Download the Brella app now from your app store." and provides links for the App Store and Google Play. Below this is a section titled "FRAUD PROTECTION" with a sub-header "INSTANT TRANSACTION CONTROL". The text explains that Brella sends alerts for potentially fraudulent activity and lists examples: "Purchases exceeding cardholder-defined thresholds", "Card-not-present debit transactions via phone, Internet or mail", and "Suspicious or high-risk transactions". It concludes with "Early warning is key. When you are aware of suspicious activity, you can contact Marion County Bank or Shazam Falcon Fraud Manager sooner." To the right of the text are three large buttons: "BILL PAY", "DEMOS & HOW TO'S", and "MOBILE BANKING". A search bar is located at the top right of the content area.

See <https://www.marioncountybank.com/personal/card-services/shazam-bolts.html#fraud-protection>.

21. If a consumer looks for the Brella by Shazam app² in Google Play or the App Store, as encouraged by the Fidelity or Marion County Bank websites, there is nothing to suggest any license or other connection between Shazam and FICO. Instead, it is described as “powered by SHAZAM.”

22. This use of “Falcon” by multiple third parties has been with FICO’s knowledge and acquiescence. The usage is pervasive, has been ongoing for years, and is squarely within FICO’s claimed financial fraud management field of use. Further, CrowdStrike produced documents to FICO on April 26, 2019, depicting these and many other third party usages for various goods and services competitive with or related to those identified in the ‘549 Registration, and provided further evidence of third party usage when CrowdStrike filed its Amended Petition for Cancellation or Amendment in the consolidated proceedings on July 22, 2019. FICO has not caused these third parties to stop or modify their usage to control use of FALCON, to address the deception caused by these third party usages, or to address the loss of significance of FALCON as a mark that is caused by these usages. To the contrary, on information and belief, the number of third party usages has only increased over the past fifteen plus months. Additional examples of third party usages are attached hereto as **Exhibit B**. FICO’s course of conduct has caused the claimed FALCON mark to lose significance as an indicator of source, and FICO has known about and acquiesced to these uses.

² Brella by Shazam is the new name for the Shazam Bolt\$ app, according to Shazam’s website at <https://www.shazam.net/news/company-news/coming-soon-shazam-bolt-mobile-app-name-change-to-brella/>.

23. Numerous uncontrolled third-party uses have resulted in the FALCON mark losing significance as a mark and ceasing to function as an indication of source, and/or result in the term “Falcon” becoming generic for, at the very least, the products and services identified in the ‘549 Registration.

CANCELLATION OF THE ‘549 REGISTRATION

Abandonment – 15 U.S.C. § 1127

24. CrowdStrike incorporates and realleges here as if fully set forth the allegations in paragraphs 1 through 23 in this Petition for Cancellation.

25. FICO has abandoned its claimed FALCON mark by allowing widespread, uncontrolled use of “Falcon” by third parties to refer to goods and services similar or identical to those identified in FICO’s ‘549 Registration. FICO has known about and acquiesced to these third-party uses. The result is loss of significance of FALCON as a mark, abandonment and/or invalidity.

26. The widespread third-party use of “Falcon” to refer to goods and services similar or identical to those identified in the ‘549 Registration confirms that FICO has failed to exercise adequate control over the use of the claimed FALCON mark. The uncontrolled and proliferating third-party use of “Falcon” in connection with goods and services covered by the ‘549 Registration has resulted in the loss of significance of the claimed FALCON mark and failure to function as a mark.

27. Even if FICO licensed or licenses such third-party uses of the claimed FALCON mark, FICO has failed to exercise adequate control, including over the promotion and provision of the goods and services, to maintain trademark rights. FICO’s failure to exercise adequate control has caused and will continue to cause deception, constitutes naked licensing and resulted

in abandonment. FICO's course of conduct has caused the claimed FALCON mark to lose significance as a mark.

28. Alternatively, the extensive third-party uses of "Falcon" have caused the term to become generic for the products and services identified in the '549 Registration.

29. For these reasons, and those set forth above, FICO's claimed FALCON mark fails to function as a trademark and the '549 Registration should be cancelled in its entirety.

WHEREFORE, CrowdStrike will be damaged by the continued registration of Registrant's FALCON mark as shown in the '549 Registration, and prays that:

1. The '549 Registration be cancelled in its entirety due to abandonment.
2. That any such further relief be granted to CrowdStrike as may be deemed reasonable and appropriate.

Petitioner hereby authorizes the charge of any and all fees in connection with this Petition to Deposit Account No. 134520.

Respectfully submitted,

Date: August 13, 2020

By: /s/ Carla B. Oakley

Carla B. Oakley
Jenna K. Stokes
Morgan, Lewis & Bockius LLP
One Market, Spear Street Tower
San Francisco, CA 94105
carla.oakley@morganlewis.com
jenna.stokes@morganlewis.com
Telephone: (415) 442-1301
Facsimile: (415) 442-1001

Ryan Tyz
Erin Jones
Tyz Law Group PC
4 Embarcadero Center, Suite 1400
San Francisco, CA 94111
rtyz@tyzlaw.com

ejones@tyzlaw.com
Telephone: (415) 849-3578

Attorneys for CrowdStrike, Inc.

EXHIBIT A

United States of America

United States Patent and Trademark Office

CROWDSTRIKE FALCON

Reg. No. 4,629,491

Registered Oct. 28, 2014

Int. Cls.: 9 and 45

TRADEMARK

SERVICE MARK

PRINCIPAL REGISTER

CROWDSTRIKE, INC. (DELAWARE CORPORATION)
15440 LAGUNA CANYON ROAD, SUITE 250
IRVINE, CA 92618

FOR: DOWNLOADABLE COMPUTER SOFTWARE FOR COMPUTER AND NETWORK SECURITY, IN CLASS 9 (U.S. CLS. 21, 23, 26, 36 AND 38).

FIRST USE 2-24-2014; IN COMMERCE 2-24-2014.

FOR: MONITORING OF COMPUTER SYSTEMS FOR SECURITY PURPOSES; PROVISION OF SYSTEMS FOR THE MANAGEMENT OF COMPUTER AND NETWORK THREATS, NAMELY, SURVEILLANCE AND MONITORING OF VULNERABILITY AND SECURITY PROBLEMS IN COMPUTER HARDWARE, NETWORKS, AND SOFTWARE; IMPLEMENTING PLANS FOR IMPROVING COMPUTER AND NETWORK SECURITY FOR BUSINESSES AND GOVERNMENTAL AGENCIES, NAMELY, COMPUTER SECURITY ASSURANCE, ADMINISTRATION OF DIGITAL KEYS AND DIGITAL CERTIFICATES, PROVIDING FRAUD DETECTION SERVICES FOR ELECTRONIC FUNDS TRANSFER, AND CREDIT AND DEBIT CARD AND ELECTRONIC CHECK TRANSACTIONS VIA A GLOBAL COMPUTER NETWORK, IN CLASS 45 (U.S. CLS. 100 AND 101).

FIRST USE 5-18-2013; IN COMMERCE 5-18-2013.

THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

OWNER OF U.S. REG. NO. 4,336,365.

SN 85-982,701, FILED 2-7-2013.

TARAH HARDY, EXAMINING ATTORNEY



Michelle K. Lee

Deputy Director of the United States
Patent and Trademark Office

United States of America

United States Patent and Trademark Office

CROWDSTRIKE FALCON

Reg. No. 4,720,653

Registered Apr. 14, 2015

Int. Cl.: 42

SERVICE MARK

PRINCIPAL REGISTER

CROWDSTRIKE, INC. (DELAWARE CORPORATION)
15440 LAGUNA CANYON ROAD, SUITE 250
IRVINE, CA 92618

FOR: COMPUTER CONSULTATION; CONSULTING IN THE FIELD OF INFORMATION TECHNOLOGY; COMPUTER CONSULTATION IN THE FIELD OF COMPUTER AND NETWORK SECURITY; COMPUTER SECURITY CONSULTANCY IN THE FIELD OF SCANNING AND PENETRATION TESTING OF COMPUTERS AND NETWORKS TO ASSESS INFORMATION SECURITY VULNERABILITY; SOFTWARE AS A SERVICE (SAAS) SERVICES FEATURING SOFTWARE IN THE FIELD OF COMPUTER AND NETWORK SECURITY; SOFTWARE AS A SERVICE (SAAS) SERVICES, NAMELY, HOSTING SOFTWARE FOR USE BY OTHERS FOR DETECTING, BLOCKING, AND REMOVING COMPUTER VIRUSES AND THREATS; APPLICATION SERVICE PROVIDER (ASP) FEATURING NON-DOWNLOADABLE COMPUTER SOFTWARE FOR USE IN COMPUTER AND NETWORK SECURITY; MAINTENANCE AND UPDATING OF COMPUTER SOFTWARE RELATING TO COMPUTER AND NETWORK SECURITY AND PREVENTION OF COMPUTER RISKS; COMPUTER SECURITY CONSULTANCY, NAMELY, DEVELOPING PLANS FOR IMPROVING COMPUTER AND NETWORK SECURITY FOR BUSINESSES AND GOVERNMENTAL AGENCIES; CLOUD COMPUTING FEATURING SOFTWARE FOR USE IN COMPUTER AND NETWORK SECURITY; CLOUD COMPUTING SERVICES IN THE FIELD OF COMPUTER AND NETWORK SECURITY; COMPUTER SERVICES, NAMELY, ACTING AS AN APPLICATION SERVICE PROVIDER IN THE FIELD OF KNOWLEDGE MANAGEMENT TO HOST COMPUTER APPLICATION SOFTWARE FOR CREATING DATABASES OF INFORMATION AND DATA RELATED TO MALWARE AND COMPUTER AND NETWORK SECURITY; COMPUTER SERVICES, NAMELY, ONLINE SCANNING, DETECTING, QUARANTINING, AND ELIMINATING VIRUSES, WORMS, TROJANS, SPYWARE, ADWARE, MALWARE AND UNAUTHORIZED DATA AND PROGRAMS ON COMPUTERS, NETWORKS, AND ELECTRONIC DEVICES; COMPUTER SYSTEMS ANALYSIS; IMPLEMENTING PLANS FOR IMPROVING COMPUTER AND NETWORK SECURITY AND PREVENTING CRIMINAL ACTIVITY FOR BUSINESSES AND GOVERNMENTAL AGENCIES, NAMELY, IDENTIFYING MALWARE ON COMPUTER SYSTEMS, IDENTIFYING THE SOURCE AND GENEALOGY OF MALWARE, AND IDENTIFYING THE OBJECTIVES OF COMPUTER SYSTEM ATTACKERS, IN CLASS 42 (U.S. CLS. 100 AND 101).



Michelle K. Lee

Director of the United States
Patent and Trademark Office

FIRST USE 3-0-2014; IN COMMERCE 3-0-2014.

Reg. No. 4,720,653 THE MARK CONSISTS OF STANDARD CHARACTERS WITHOUT CLAIM TO ANY PARTICULAR FONT, STYLE, SIZE, OR COLOR.

OWNER OF U.S. REG. NO. 4,336,365.

SN 85-843,788, FILED 2-7-2013.

TARAH HARDY, EXAMINING ATTORNEY

EXHIBIT B



Online Banking Login

Username

Username Password

Password

- [COVID-19 Statement from President](#)
- [Online and Mobile Banking](#)
- [Demo](#)
- [Personal Enroll](#)
- [Commercial Enroll](#)
- [E-Statements](#)
- [Rates](#)
- [Transfer the Cents](#)

Introducing Brella



The mobile app that lets you track your account & receive fraud alerts on your smartphone or tablet!

[Learn More](#)

ATM / Debit Cards w/Falcon Fraud

[Home](#) > [Other Services](#) > ATM / Debit Cards w/Falcon Fraud

Central State Bank debit cards look like a credit card but work like a check. Our debit cards are accepted where Visa is accepted and they can also be used as an ATM card.


We are enrolled in Shazam's Falcon Fraud program to safeguard your transactions from fraud. We also offer Brella - an app that can help you monitor your card transactions by phone. You can enroll in Brella by [clicking here](#).

Central State Bank

- [Home](#)
- [Privacy Policy](#)
- [Contact Us](#)
- [USA Patriot Act](#)
- [Terms & Conditions](#)

© 2020 Central State Bank. All Rights Reserved. Website designed by [ProfitStars](#).

Member **FDIC** |

Equal Housing Lender 

**LOGIN**

Online Banking

Login ID

LOGIN

Sign Up

(https://online.todaysbank.com/todaysbk_onlineE2E/enroll.html#/login)

Forgot Password?

(<https://online.todaysbank.com/todaysbankonline/uux.aspx#/login/resetPasswordUsername>)



Debit Card Tips

The advantages of having a debit card linked to your checking account are numerous. From making shopping in-store and online convenient to protecting against the risk of carrying (and losing) cash, it just makes good “financial sense” to have a debit card. Whether you are getting started in banking or just looking to learn a few new things, here are some tips that can help every debit card user.

1. Be Security Minded

Debit cards are a wonderful convenience; however, convenience comes with risks. Be sure to keep your card in a safe place at all times, be aware of debit card scams, and use your card with vendors (online or in person) that you trust. Even the most diligent person can still have an instance of debit card fraud. Catching it early is important. Monitor your accounts regularly and report any suspicious activity.

2. Be prepared.

It is inevitable. It can happen to even the most careful and organized person. Misplacing or having your debit card stolen is inconvenient; however rest assured that you can quickly cancel your card to protect against any unauthorized access to your checking account funds.

But wait a minute.... how are you supposed to do that if you don't have the card?!

That is why we recommend storing these important phone numbers so that you can quickly access them should you ever need to.

Lost or Stolen Debit Card:

- Contact Today's Bank at (479) 582-0700 during business hours to cancel your card and to have a new card issued.
- Verify your transactions with a Today's Bank Representative.
- A bank representative will process any disputes, give provisional credit back for fraudulent transactions, and order your new card.
- After business hours, call Shazam at (800) 383-8000 to report the card lost or stolen.

SHAZAM Privileged Status® Bank

Today's Bank is a SHAZAM Privileged Status® Bank. Privileged Status® cardholders should look for ATMs that display the Privileged Status® logo to avoid ATM surcharges when using any ATM in the Shazam Privileged Status® Network. Visit our **location page (/about/locations)** for ATM Privileged Status locations near you.

Remember you can always get "cashback" as you're making a purchase with your debit card. Most retail, grocery and convenience stores provide this option at no charge. Simply ask the cashier before you complete your transaction. As an example, if you were buying a pack of gum and bottle of water totaling \$1.75 and you requested \$20 cashback, the total transaction amount debited to your checking account would be \$21.75.

Keep in mind, stores may have different limits to how much "cashback" you can get through this method.

Debit Card Features

SHAZAM Falcon Fraud Manager

Protecting you from unauthorized use of your debit card is one of our top priorities at Today's Bank. Today's Bank has a monitoring system to mitigate fraud called SHAZAM Falcon Fraud Manager to help guard your debit card against fraudulent activity. If suspicious activity is detected on your card, you will be contacted by a bank employee or a Falcon fraud specialist calling on the bank's behalf to verify the transactions in question. If you get a call or a text message from a fraud specialist or your card is being denied after normal business hours, please contact Falcon Fraud 24/7 support at (866) 508-2693.

How Does Falcon Work?

- Monitors all card transactions for unusual or suspicious activity
- Takes into account your normal activities
- Each transaction is scored based on the likelihood of fraud
- Depending on the score, once an unusual or suspicious transaction takes place, you will be receiving a call or text message and/or the account will have a temporary block put on it until you can be contacted.

How Am I Notified?

During the notification process, the fraud specialist from Falcon will note that he or she is calling on behalf of Today's Bank. The fraud specialist will ask you to validate your identity via a series of qualifying questions that must exactly match the information in our records to successfully authenticate your identity.

Please remember that no one will ask for your personal identification number (PIN) or 3 digit security code located on the back of your card to verify your identity. Always use caution when providing your card information, and contact us if you suspect your card has been stolen or compromised. If you cannot be reached, Falcon may put a temporary block on your account to prevent further fraudulent activity.

What Do I Need to Do?

To ensure that we can reach you promptly if fraudulent activity is suspected, we need to have current contact information on file to include:

- Primary phone number
- Secondary phone number (mobile phone or work number)
- Current address
- City, State and ZIP code

It is very important to keep this information current. If your information changes, **please contact us (/about/contact-us)** at (800) 945-0073. **Remember Today's Bank will never ask you for your debit card or cash card number, or the PIN or CVV.**

Brella (formerly Shazam BOLT\$)

Brella is a service provided to Today's Bank customers to protect against debit card identity theft. By downloading the Brella Mobile App, you can:

- View a primary debit card account's balance information
- Acquire various transaction alerts
- Fraud Alerts 24/7
- Find an ATM near you with ATM Locator
- Login with Touch ID for faster, easier access to your account.

To enroll in Brella click here. (<https://bolts.shazam.net/ShazamWebPortal/index.php>)

MyPic Debit Card

Express your personality with a Today's Bank Debit Card. **Customize your debit card (/tools/custom-debit-card)** by choosing your own photo for only \$5. You can choose from our gallery of photos, or upload your favorite photo. Make your card more secure and fun with a photo. Get personal with your custom debit card from Today's Bank.



(/calculators)

Calculators

(/calculators)



(<https://online.todaysbank.com>

/todaysbk_onlineE2E

/enroll.html#/login)

Enroll in Online Banking

(<https://online.todaysbank.com>

/todaysbk_onlineE2E

/enroll.html#/login)



Find a Location

(/about/locations)



TODAY'S BANK
(/)

PO Box 667
Huntsville, AR 72740

(800) 945-0073

Routing #:
082901745

Bank

About Us (/about/about-us) | [Contact Us \(/about/contact-us\)](#) | [Locations \(/about/locations\)](#) | [Forms \(/tools/forms\)](#) | [Switch Kit \(/tools/switch-kit\)](#) | [Accessibility \(/accessibility\)](#)

Disclosures (/e-banking/disclosures) | [Privacy Policy \(/privacy-policy\)](#) | [Terms of Service \(/terms-of-service\)](#) | [NMLS #341187](#)

Facebook (/facebook) | [Twitter \(/twitter\)](#) | [Instagram \(/instagram\)](#) | [LinkedIn \(/linkedin\)](#)

[Back to Top](#)

©2020 Today's Bank

[\(\)](#)[LOGIN](#)[Menu](#)

Debit Cards

Report a Lost or Stolen Debit Card

During business hours: Please call us immediately at (573) 722-3517

After business hours: Please call SHAZAM® Card Services at (800) 383-8000

Mastercard® Debit Card

Mastercard® Debit Cards give you a fast and convenient way to buy the products and services you need without having to write a check or carry cash. Contact your local branch to request a Bank of Advance debit card and choose from the following card images. **Call (800) 717-4923 to activate your card and establish your PIN.**



Baseball



Beach



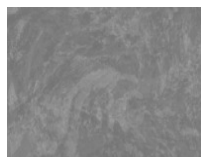
Cow



Deer



Flag



Grey Marble



Hay Field



Jade



Leather



Map



Regal



Wheat Field



White Marble



White Texture



Overdraft Protection for Debit Cards

Debit card transactions that will overdraw your account will be declined unless you request and authorize overdraft protection for your debit card, which is an optional feature of Bounce

Protection. If you choose to activate overdraft protection for your debit card, we will pay debit card transactions that overdraw your account in accordance with **Bounce Protection limits (/personal/bounce-protection)**. You will be assessed the standard overdraft fee of \$24.00 per transaction. You are never charged unless you use the protection. You can accept or decline this service at any time by contacting your local branch.

Brella™ (Previously SHAZAM® BOLT\$™)

Brella™ acts like a high-tech, early-warning system that immediately alerts you to potentially fraudulent activity by sending you alerts regarding your debit card purchases. With the help of Brella, no one is better equipped to catch debit card fraud than you. After all, you know what you've purchased and can spot unauthorized transactions instantly.

Customize your alert settings to notify you when purchases exceed a preset amount, transactions occur in a foreign country, or your debit card number is used but your card is not present, such as telephone or internet purchases. You can also check your account balance information anytime, anywhere.

Brella gives you more control over your debit card. If your card is stolen or missing, you can **pause your card** without affecting previous transactions. With just the tap of a button, block or unblock your own card to protect yourself from possible fraud. You can also easily **submit a travel notice** to help ensure uninterrupted debit card access when you're on the road.

To register your card and set up your alerts, download the Brella Card Manager app from the Apple App Store, Google Play Store or **go to the Brella website (<https://shazambrella.net>)**. You can also access Brella from the convenience of your Bank of Advance Mobile Banking app*. After registering your debit card, be sure to customize your alerts to be notified every time your debit card is used.

Fraud Detection

To protect your account, Bank of Advance along with the SHAZAM® Falcon Fraud Manager, monitor your debit card transactions for potentially fraudulent activity. This may include a sudden change in location, unusually costly purchases, or any pattern associated with new fraud trends. If suspicious activity is detected on your debit card, you will receive a text alert from **72718**. Reply Yes or No to confirm or deny the activity. If you don't reply to the text or your phone number is not a mobile number, you will receive an automated voice call from **855-219-5399**. Save these numbers to your contacts so you don't miss any alerts! A temporary block may be placed on your card if verification cannot be made. To assure your card is not blocked unnecessarily, please keep your phone numbers up to date.

If you are going to be traveling, please contact your local branch so we can make SHAZAM Falcon Fraud Manager aware of your location.

ATM Locations

Bank of Advance ATM Locations

- Bank of Advance – 105 E Gabriel, Advance, MO
- Chaffee Banking Center – 102 E Yoakum, Chaffee, MO
- Dexter Banking Center – 1428 W Business Hwy 60, Dexter, MO
- Bowen Banking Center – 415 W 5th St, Bowen, IL

Nationwide ATM Locations

Bank of Advance participates in **MoneyPass® ATM Network (<https://www.moneypass.com/index.html>)** and **SHAZAM® Privileged Status ATM Network (<https://www.shazam.net/index.html>)**. MoneyPass and Shazam Privileged Status offer surcharge-free ATM usage around the country. A surcharge is a fee charged to cardholders by the owner of the ATM. With a Bank of Advance debit card, you can use any ATM in these networks without paying a surcharge*. Click the links to find an in-network ATM location near you.

MoneyPass ATM Network offers a free mobile app in order to easily search for in-network ATMs on your mobile device. Visit your app store to download the MoneyPass app today!

*\$1.00 Bank of Advance Foreign ATM Fee may still apply.



ATM Safety

Approaching the ATM

- Avoid dark or remote locations
- Take another person with you if possible
- Keep your doors locked and passenger window closed

Using the ATM

- Block the view of others by cupping your hand over the keypad
- Quickly remove your cash, receipt and card from the ATM
- Pocket cash immediately

Preventing Debit Card Fraud

- Memorize your PIN - **Do NOT write it on your card!**
- Do not tell anyone your PIN or account number
- Do not loan your card to anyone
- Report lost or stolen cards immediately
- NEVER give your PIN over the phone

** You must be an Online Banking customer to access the Mobile Banking app.*

Connectivity and usage rates may apply. Contact your wireless provider for more details.

The iPhone®, iPad®, App Store and Apple logo are all trademarks of Apple, Inc., registered in the U.S. and other countries. Android™

and Google Play are trademarks of Google Inc.



Get Cash on the Road

Follow where the road takes you and find in-network ATMs along the way.

ATM Locator (<https://www.moneypass.com>)

f(<https://www.facebook.com/bankofadvance/>) **ir**
 (<https://www.linkedin.com/company/bank-of-advance>) **tw**
 (<https://twitter.com/BankofAdvance>)

**Banno
Monitor™**
 Verified: Aug 11, 2020

GeoTrust (<https://smarticon.geotrust.com/smarticonprofile?Referer=https://www.bankofadvance.com>)

Security (/security)

Privacy (/privacy-policy)

Disclosures (/disclosures)

© 2020 Bank of Advance. Member FDIC (<https://www.fdic.gov/>).
 Equal Housing Lender (<https://portal.hud.gov/hudportal/HUD>)



[Q Ask](#)[Member login](#)

username

Go

[Forgot username](#) [Enroll](#) →**Routing Number: 307070034**[Blue Federal Credit Union](#) ≡

Falcon Fraud

[Home](#) [Why Blue?](#) » [The Blue Difference](#) » [Fraud Protection](#) » *Falcon Fraud*

Automated fraud protection

As part of our continuing effort to bring the best technology and service to our members, Blue Federal Credit Union will be upgrading its Fraud Detection and Notification System starting March 31, 2015. The new system will provide more immediate attention to our members when fraud is suspected. The notification portion of the system includes a state-of-the-art automated assistant to help our members review transactions and confirm their spending activity on their Blue debit card.

If you receive a notification call from our automated assistant, whom we have nick-named Jill, please work with her to answer questions regarding your recent card activity. It is very important to note that although these calls will now be automated and no longer conducted by a live person, we will NEVER ask for sensitive information. This means we will never ask you to identify yourself with information like your social security number, debit card number, or PIN. If you are asked to provide this information, hang up the phone and call us at 1-800-368-9328 to see if your account is threatened by a fraud attempt.

If you are suspicious of a transaction identified through Jill, your call will be transferred to our outstanding member support team at Card Member Security who will help you take necessary precautions to protect your cards and other related accounts. If the recent activity is legitimate, you will be able to close the case with Jill using your touch-tone phone.

Get answers to your questions.

If you have any questions at all, please contact us at 1-800-368-9328 or stop into any of our branches to speak with a members services representative. Thank you for your continued membership and helping us protect your accounts to the highest level of security possible.

[Find a branch](#)

Life happens.

Help pay for all of life's curve balls with a personal loan. We have easy, low payments!

[Learn more](#)[Facebook](#) [Twitter](#) [instagram](#) [linkedin](#) [youtube](#) [Triangle](#) [Apple](#)



Falcon Fraud

January 9, 2017 by HomeTown

Falcon Fraud is a product HomeTown Bank uses through our debit card provider, Shazam. It helps identify and reduce fraud risk by detecting potentially fraudulent PIN and signature-based debit transactions that could be run through your debit card.

Falcon Fraud works by identifying transactions based on a pre-determined set of parameters that appear to be suspicious. If a transaction goes through that is suspicious, Shazam will directly contact the customer to determine if the transaction is valid or not.

If they do not have a successful call attempt, Shazam will put a temporary block on the debit card to prevent further fraudulent activity to protect both the customer and the bank.

Traveling could flag fraudulent activity on your account if you do not let your local HomeTown Bank know you will be traveling with your debit card. Here are some steps to take when traveling so your card isn't marked as fraudulent and blocked:

- ✔ Notify bank of travel destinations and dates before you travel
- ✔ Verify current contact information with the bank.
- ✔ PIN transactions are more secure and are less likely to be flagged for fraud.
- ✔ Always carry alternate means of payment in case your card were to be blocked.
- ✔ Download Brella Card Manager from your app store to receive debit card notifications to your smartphone.

If your card is blocked due to fraudulent activity, you can contact Shazam directly at (866) 508-2693 or your local HomeTown Bank to take further action to get your card unblocked.

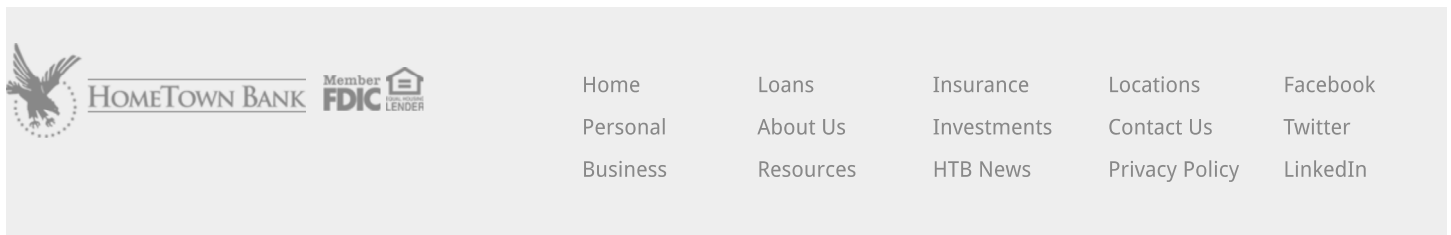
The graphic is for the STAR SAVERS program. It features two cartoon children, a boy and a girl, on the left. The text 'HOME TOWN BANK' is at the top, followed by 'STAR SAVERS' in large, bold letters. Below that, it says 'Rewards Parents Will Love! Education for a Lifetime!'. On the right, there are five circular icons representing different rewards: 'Young Savers 3.5% APY', 'Service Stars \$2/hr', 'Great Grades \$2 per \$100', 'Learn & Earn \$10 per \$100', and 'College Scholarship'. The background is dark green with a pattern of stars and money symbols.

HomeTown News

COVID-19 Response

Update 7/23/2020: With the Governor's Executive Order mandating face masks, beginning Saturday, July ... [\[Read More...\]](#)

[More from HomeTown News](#)



Fraud Protection

[Home](#) > [Personal](#) > [Debit Cards](#) > [Fraud Protection](#)



You're Covered!

Iowa State Bank protects your debit card with Falcon Fraud Manager.

What is Falcon?

Falcon is fraud prevention software from SHAZAM, our debit card provider that helps identify and reduce fraud risk by detecting potentially fraudulent PIN-based and signature-based debit transactions. It has a proven reputation of helping minimize payment card fraud losses.

How does Falcon work?

Falcon reviews how and where your card is being used and scores transactions based on transaction data and cardholder profile factors. Each transaction is given a score from one to 999, and the higher the score, the greater the likelihood that the transaction is fraudulent.

What happens if Falcon detects fraudulent activity on my debit card?

SHAZAM Fraud Specialist will call you if any suspicious activity is detected on your account. They will identify themselves as SHAZAM, calling on behalf of Iowa State Bank. If they are unable to reach you, they will leave a message with their contact information.

Fraud Text Alerts: When a suspicious transaction takes place on your account, you will receive a text alert within seconds. You can then confirm or deny the activity with a **Yes** or **No** response via text message. If the system doesn't receive a text response from you or the phone number isn't a mobile number, it will attempt to contact you via an automatic voice call, to which you may also respond with a **Yes** or **No**.

Falcon Fraud Manager maintains a 24/7 watch on your account. On high risk activity scenarios they will suspend activity immediately on your debit card until they can talk to you to determine if the risk is fraudulent activity or not. This process has saved our customers thousands of dollars in potential loss.

What information will I be asked for?

SHAZAM will ask you to verify your address. Once your address has been verified, they will then ask you to confirm your purchase activity.

Will I be asked for my personal information?

No. SHAZAM will never ask for your personal information, such as the last four digits of your Social Security number, security codes, etc. SHAZAM will only ask for verification of your address.

Does this service cost anything for me?

No. Iowa State Bank wants you to use your debit card with confidence. Falcon Fraud Manager is a FREE protection service available to you.

What if my debit card is declined at a merchant location?

One of the reasons may be that it was flagged as highly likely to be fraud, based on the way you typically use your card. If your transaction is declined for that reason, you will receive a phone call from a SHAZAM Fraud Specialist to verify the transaction. If it was a legitimate transaction, the details will be made part of your card profile so that these types of transactions have a greater chance of being approved in the future.

How can I be proactive when using my debit card with Falcon Fraud Manager?

One thing to keep in mind is Falcon Fraud Manager will immediately block your card if it detects suspicious activity. A few tips to keep in mind are:

1. Always let Iowa State Bank know when you plan to travel out of state and out of the country. This can help avoid potential blocks on your debit card allowing you to use it more freely.
2. In case your debit card is blocked from fraudulent transactions, we recommend always carrying multiple forms of payment with you.

Tips for preventing card fraud on your account...

- Memorize your PIN. Don't write it on your card or anything you carry near your card.
- Don't tell anyone your PIN or account number.



- Don't loan anyone your card.
- Report lost or stolen cards immediately. You may be liable for activity on your card if you do not report it as lost or stolen.
- NEVER give your PIN over the phone, especially cellular phones.
- NEVER respond to a link or phone number in an e-mail message requesting personal information. Phishers often use this scam to trick you into divulging personal data



Customer Service

Contact Us: jsboc@iowastatebank.net

[View Locations Info.](#)

[Real Estate Agency](#)

[Insurance Agency](#)

[Lost or Stolen Debit Card](#)

[Personal Checks Reorder](#)

[Business Checks Reorder](#)

Routing#: 073922432

About Us

[President's Letter](#)

[Employment Opportunities](#)

[Mission Statement](#)

[Our Blog](#)

[Our History](#)

[COVID-19 Update](#)

Locations

[Hull](#)

[Ireton](#)

[Le Mars](#)

[Orange City](#)

[Paullina](#)

[Remsen](#)

[Sanborn](#)

[Sheldon](#)

Our Top Pages

[Online Banking](#)

[Hull](#)

[Orange City](#)

[Sheldon](#)

[Locations](#)

© 2020 Iowa State Bank . All rights reserved.

[Privacy Policy](#) | [Sitemap](#) | [Terms of Use](#) | [Patriot Act](#) | [Website Accessibility Notice](#)

Custom web solutions by [VGM Forbin](#)



[JOIN FEDCHOICE](#) [ABOUT US](#) [LOCATIONS](#)

Search...

eBANKING**REGISTER FOR
NEW ONLINE BANKING**

username

LOG IN[Checking & Savings](#)[Credit Cards](#)[Loans](#)[Financial Guidance](#)[eServices](#)[Retirement Planning](#)**ALERT**

FedChoice is here to help! Our Advisors are ready and willing to assist. Click "Alert" for information on our Branch Hours and more.

[Print](#)[Email](#)[Share](#)

FRAUD PREVENTION

Online banking should be free of Internet security worries. You'll be happy to know that we are constantly updating our Web site with the latest protections and security features. Below are some links to help you learn how to make your online banking experience safe and secure.

Verified by Visa®

Get an extra layer of security when you shop online

In addition to our other ways of preventing, detecting, and resolving fraud, we offer Verified by Visa, a free, simple-to-use service that confirms your identity with an extra password when you make an online transaction.

How it works

1. Activate the Verified by Visa feature

Enroll your credit or debit card in the Verified by Visa program now, on your participating card issuer's website or while shopping online.

2. Shop at participating online merchants

Visit online merchants that display the Verified by Visa symbol for an added layer of protection.

3. Enjoy enhanced security

Enjoy added peace of mind. Activate Verified by Visa on your Visa credit and debit cards.

Nationwide Identity Theft

How does Nationwide® identity theft coverage work?

Fast! Just make one call to our identity theft hotline. Our identity theft experts will immediately take action to:

- Quickly assess your situation to determine if fraud has occurred.
- Stop damage to your credit within minutes of your authorization by directly contacting major credit bureaus.
- Make all required phone calls to creditors, banks and agencies.
- Assist you in replacing documents including driver's license, passport, social security card or other ID.
- Provide an emergency cash advance if theft occurs while you're away from home (restrictions and limits apply).
- Provide up to \$25,000 in recovery for expense reimbursement with no deductible.
- And provide a full host of Identity Theft protection services to save you time, money, and frustration.

Now with free Credit Monitoring!

Nationwide's teamed up with Worldwide Assistance® and TransUnion® to offer ID theft customers free Credit Monitoring! This optional service sends e-mail alerts when your credit report changes. Best of all, it's free with the purchase of identity theft coverage from Nationwide!

Don't spend countless hours trying to recover your stolen identity. Save time, money, and frustration with identity theft coverage from Nationwide, your identity theft protection company.

To learn more about Identity Theft Coverage, **contact a local agent today!**

Real-Time Decisioning

We have enhanced our fraud detection system to better protect your credit and debit cards. A sophisticated network makes "Real-Time Decisions" based on your usual spending patterns. If an "out of character" transaction is made, an alert will be created and you will be contacted immediately for verification.

This Falcon fraud detection service provides another weapon in the ongoing battle against unauthorized use of plastics. In literally seconds, the service prevents fraud by denying transactions with the possibility that the fraudster is still at the point-of-sale.

Here is an example of a how Real-Time Decisioning works:

1. A new authorization (on your debit/credit card) is attempted at the point-of-sale.
2. The transaction passes through the Real-Time Authorization Settings to determine if the transaction appears to be high-risk.

3. If the transaction passes through Authorization, it is deemed “normal” and the transaction will continue as usual.

- If it is deemed “high-risk”, the transaction is run through Real-Time rules to determine if the transaction falls outside of your usual spending patterns.
- If the Real-Time rules confirm the transaction is high-risk, an alert is created.
- Fraud is then stopped at the point of sale.
- An FIS Loss Prevention Fraud Analyst or automated voice system attempts to contact the cardholder.
- When the cardholder is reached and confirms that the transaction is indeed fraudulent, the account is blocked to prevent further activity.

Other Things to Consider

Possible Impact on You

- A small number of legitimate transactions will be declined until the validity of certain transactions may be confirmed.
- If the Fraud Analyst cannot contact the cardholder, a temporary block is placed on the account.
- The block stays on the account until the cardholder advises the Fraud Team to remove it.

Helpful Hints to Prevent Temporary Blocks

- Contact FedChoice prior to using your credit or debit cards for large transactions.
- Contact FedChoice before traveling abroad or going on vacation.
- Update FedChoice with any new phone numbers.

Opt Out

Members will have the ability to opt-out from Real-Time Decisioning temporarily or indefinitely by contacting FedChoice. However, keep in mind that this service provides security features for credit and debit card use.

FedChoice is proud to offer this valuable service to all members free of charge! With Real-Time Decisioning, we can stop card fraud at the Point of Sale!

JOIN FEDCHOICE

[Membership Eligibility](#)

[Membership Application](#)

[Membership Documentation](#)

FIND LOCATION

FAVORITE LINKS

[Learn About Credit Scores](#)

[Get Your Free Credit Report](#)

[Calculators for Loans, Savings and More!](#)

[GreenPath Financial Wellness](#)

TANGERINE FOUNDATION

[Tangerine Foundation](#)

[Federal Retirement and Benefits](#)

[Latest Articles](#)

connect with
fedchoice



too many expenses?
save money now

questions?
call, click or come in



Copyright © 2019 FedChoice Federal Credit Union. All rights reserved. All information is subject to change at any time.

FedChoice Federal Credit Union is committed to providing a website that is accessible to the widest possible audience in accordance with ADA standards and guidelines.

We are actively working to increase accessibility and usability of our website to everyone. If you are using a screen reader or other auxiliary aid and are having problems using this website, please contact us at [+1-800-969-6151](tel:1-800-969-6151)

All products and services available on this website are available at all FedChoice Federal Credit Union branches.



**ONLINE BANKING**

PERSONAL BUSINESS



SHAZAMCHEK DEBIT CARDS

If your card is lost or stolen:

- *Contact Shazam 1-800-383-8000,*
- *If you need to respond to a voicemail left by our Shazam fraud center regarding a debit card transaction, call 855-219-5399,*
- *Use your Shazam Brella app to temporarily deactivate your card, or*
- *Contact Woodford State Bank directly during regular business hours for assistance.*

ShazamChek Debit Cards

Your money within reach. Faster, smarter, reliable.

- ShazamChek Debit Cards are offered for FREE with your Woodford State Bank checking account. No annual or monthly fees!
- Gives you a faster, more economical, and convenient way to buy products and services you need.
- Convenient and safer than carrying cash.
- You have an option to pick your own Easy PIN.
- Allows you to withdraw funds directly from your checking account without ever having to write a check.
- Allows you to make purchases worldwide where Mastercard is accepted.
- Gives you the ability to withdraw funds at an ATM from a Woodford State Bank checking or approved savings account. For surcharge-free ATMs, click [here](#).
- EMV smart chip technology for added security.

- Our Falcon Fraud Manager helps you to prevent debit card fraud.
 - In addition, we offer Shazam Brella - a "set it and forget it" app, that features transaction control, travel manager, the ability to send money (fees apply) and an ATM locator.
 - Mastercard Enhanced Benefits - please visit <http://www.mastercard.us/worlddebit> .
-

Shazam Brella (Formerly Shazam Bolt\$)

Your FREE "Set it and Forget it" app.

- Fingerprint and face recognition access available.
 - Quick balance feature.
 - Transaction control – lose your card after banking hours? Turn your card off if you lose it and have the power to turn it back on when you find it.
 - Alerts – “Set it” by transaction amount, internet and phone transactions, or transactions outside of the US. Have alerts sent directly to you by text message right away.
 - Ability to view suspected fraud alerts.
 - Have the power to turn card off if you suspect fraud.
 - Send money (fees apply).
 - Manage travel notices.
 - ATM locator.
-

Mastercard Enhanced Benefits

Mastercard offers additional benefits above what Woodford State Bank is liable for. These benefits include Mastercard ID Theft Protection, Extended Warranty, Satisfaction Guarantee, Mastercard Global Service, and Mastercard Airport Concierge. Please visit [Mastercard.us/WorldDebit \(http://www.mastercard.us/worlddebit\)](http://www.mastercard.us/worlddebit) for details.

ROUTING NUMBER - 075908920

NMLS ID# - 422856

PHONE NUMBER - (608) 325-7766 (tel:+16083257766)

©2020 Woodford State Bank. All rights reserved.

Bank Websites (<https://woodfordstatebank.com/external-link.php?url=www.brownbootsbankwebsites.com%2F>) by BrownBoots Interactive, Inc.



(<https://woodfordstatebank.com/external-link.php?url=www.bauerfinancial.com%2F>)